(9)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-110628
(43)Date of publication of application : 11.04.2003

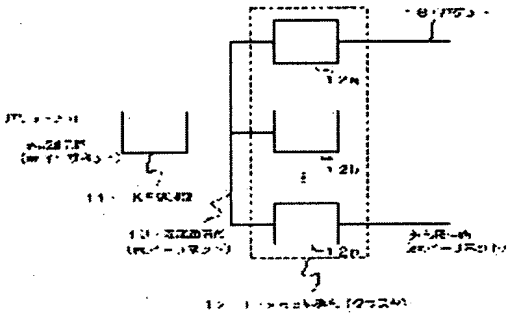
(51)Int.Cl. H04L 12/66
H04L 9/08
H04L 9/32
H04L 12/56

(21)Application number : 2001-300137
(22)Date of filing : 28.09.2001

(71)Applicant : NEC CORP
(72)Inventor : KUBO TAKUYA

(54) SECURITY GATEWAY APPARATUS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security gateway apparatus in a system for communicating encrypted packets that can prevent loads of arithmetic processing required for encrypting the packets from being concentrated so as to relieve the load for arithmetic processing in respective components.
SOLUTION: The security gateway apparatus comprises; an authentication key exchange means 11 for conducting negotiation processing to negotiate parameters required for IP security communication with an opposed security gateway; and an IP security processing means 12 connected to the authentication key exchange means 11 via an internal communication path 13 and executing IP security processing for a packet sent from the authentication key exchange means 11.



LEGAL STATUS

[Date of request for examination]	13.08.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3603830
[Date of registration]	08.10.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－110628
（P2003－110628A）
(43)公開日　平成15年４月11日(2003.4.11)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	５Ｊ１０４
9/08		12/56	Ｈ	５Ｋ０３０
9/32		9/00	６０１Ｃ	
12/56			６７５Ａ	

審査請求　有　　請求項の数21　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－300137(P2001－300137)

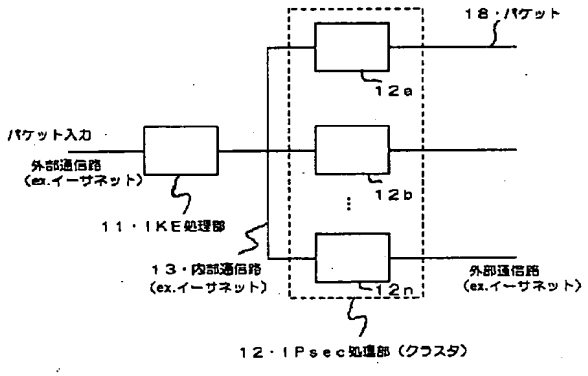
(22)出願日　平成13年９月28日(2001.9.28)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　久保　拓也
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100096105
弁理士　天野　広

Ｆターム(参考)　5J104 AA01 AA16 EA04 EA26 NA02
NA05 PA07
5K030 GA15 HA08 HB18 HD03 HD08
KA07 LE03

(54)【発明の名称】　セキュリティゲートウェイ装置

(57)【要約】
【課題】パケットを暗号化して通信を行うシステムにおいて、パケットの暗号化に要する演算処理の負荷の集中を防止し、個々のコンポーネントにおける演算処理の負荷を減少させる。
【解決手段】本セキュリティゲートウェイ装置は、ＩＰセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートするネゴシエーション処理を行う認証キー交換手段１１と、認証キー交換手段１１と内部通信路１３で接続されており、認証キー交換手段１１から送られてきたパケットに対してＩＰセキュリティ処理を実行するＩＰセキュリティ処理手段１２と、からなる。



1

【特許請求の範囲】

【請求項１】　ＩＰセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートするネゴシエーション処理を行う認証キー交換手段と、

前記認証キー交換手段と内部通信路で接続されており、前記認証キー交換手段から送られてきたパケットに対してＩＰセキュリティ処理を実行するＩＰセキュリティ処理手段と、

からなるセキュリティゲートウェイ装置。

【請求項２】　前記ＩＰセキュリティ処理手段は複数のＩＰセキュリティ処理装置からなり、

前記認証キー交換手段は、前記ネゴシエーション処理後に、前記パケットを前記複数のＩＰセキュリティ処理装置の何れかに振り分ける振り分け処理を行い、

前記複数のＩＰセキュリティ処理装置の各々は前記認証キー交換手段から振り分けられた前記パケットに対してＩＰセキュリティ処理を実行するものであることを特徴とする請求項１に記載のセキュリティゲートウェイ装置。

【請求項３】　前記認証キー交換手段は、ＩＰセキュリティ処理を行うべきパケットを受信した場合には、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットのＩＰセキュリティ処理を行うＩＰセキュリティ処理装置を決定し、前記パケットを前記ＩＰセキュリティ処理装置に転送することを特徴とする請求項２に記載のセキュリティゲートウェイ装置。

【請求項４】　前記認証キー交換手段はローカルデータベースを有しており、

前記認証キー交換手段は、検索したパラメータと、前記パケットのＩＰセキュリティ処理を行わせることに決定した前記ＩＰセキュリティ処理装置の識別子とを相互にリンク付けした状態で、前記パラメータ及び前記識別子を前記ローカルデータベースに保存することを特徴とする請求項３に記載のセキュリティゲートウェイ装置。

【請求項５】　前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記ＩＰセキュリティ処理装置に転送することを特徴とする請求項３または４に記載のセキュリティゲートウェイ装置。

【請求項６】　前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えており、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存するものであることを特徴とする請求項２乃至５の何れか一項に記載のセキュリティゲートウェイ装置。

【請求項７】　前記認証キー交換手段から前記パケットを受信した前記ＩＰセキュリティ処理装置は、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行うことを特徴とする請求項６に記載のセキュリティゲートウェイ装置。

2

【請求項８】　前記認証キー交換手段は前記パケットをカプセル化し、カプセル化した前記パケットを前記ＩＰセキュリティ処理装置に転送することを特徴とする請求項３に記載のセキュリティゲートウェイ装置。

【請求項９】　前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えており、

前記複数のＩＰセキュリティ処理装置の各々は、前記認証キー交換手段から受信したカプセル化した前記パケットを復元し、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行うことを特徴とする請求項８に記載のセキュリティゲートウェイ装置。

【請求項１０】　前記認証キー交換手段並びに前記複数のＩＰセキュリティ処理装置の各々はプロセッサを搭載した基板から構成されており、前記認証キー交換手段並びに前記複数のＩＰセキュリティ処理装置の各々は内部バスで相互に接続されていることを特徴とする請求項１乃至９の何れか一項に記載のセキュリティゲートウェイ装置。

【請求項１１】　前記認証キー交換手段と前記ＩＰセキュリティ処理手段との間におけるパケットの転送は、データリンクレイヤの種別に応じて、最適化されることを特徴とする請求項１乃至１０の何れか一項に記載のセキュリティゲートウェイ装置。

【請求項１２】　認証キー交換手段が、ＩＰセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートする第１の過程と、

前記認証キー交換手段と内部通信路で接続されているＩＰセキュリティ処理手段において、前記認証キー交換手段から送られてきたパケットに対してＩＰセキュリティ処理を実行する第２の過程と、

からなるパケットに対するＩＰセキュリティ処理方法。

【請求項１３】　前記ＩＰセキュリティ処理手段は複数のＩＰセキュリティ処理装置からなり、

前記第１の過程の後に、前記認証キー交換手段が、前記パケットを前記複数のＩＰセキュリティ処理装置の何れかに振り分ける第３の過程をさらに備え、

前記第２の過程においては、前記複数のＩＰセキュリティ処理装置の各々が前記認証キー交換手段から振り分けられた前記パケットに対してＩＰセキュリティ処理を実行するものであることを特徴とする請求項１２に記載のパケットに対するＩＰセキュリティ処理方法。

【請求項１４】　前記認証キー交換手段が、ＩＰセキュリティ処理を行うべきパケットを受信した場合に、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索する第４の過程と、

検索したパラメータに基づいて、前記パケットのＩＰセキュリティ処理を行うＩＰセキュリティ処理装置を決定する第５の過程と、
前記パケットを前記第５の過程において決定した前記ＩＰセキュリティ処理装置に転送する第６の過程と、
を備えることを特徴とする請求項１３に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項１５】　前記認証キー交換手段はローカルデータベースを有しており、
前記認証キー交換手段が、検索したパラメータと、前記パケットのＩＰセキュリティ処理を行わせることに決定した前記ＩＰセキュリティ処理装置の識別子とを相互にリンク付けする過程と、
前記認証キー交換手段が、前記パラメータ及び前記識別子を前記ローカルデータベースに保存する過程と、
を備えることを特徴とする請求項１４に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項１６】　前記第６の過程において、前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記ＩＰセキュリティ処理装置に転送することを特徴とする請求項１４または１５に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項１７】　前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えており、
前記複数のＩＰセキュリティ処理装置の各々が、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存する過程を備えることを特徴とする請求項１３乃至１６の何れか一項に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項１８】　前記認証キー交換手段から前記パケットを受信した前記ＩＰセキュリティ処理装置が、前記ローカルデータベースから、前記パケットに対応するパラメータを検索する過程と、
前記ＩＰセキュリティ処理装置が、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行う過程と、
を備えることを特徴とする請求項１７に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項１９】　前記認証キー交換手段が前記パケットをカプセル化する過程を備えており、
前記カプセル化された前記パケットが前記第６の過程において前記ＩＰセキュリティ処理装置に転送されることを特徴とする請求項１４に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項２０】　前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えており、
前記複数のＩＰセキュリティ処理装置の各々が、前記認証キー交換手段から受信したカプセル化した前記パケットを復元する過程と、
前記複数のＩＰセキュリティ処理装置の各々が、前記ローカルデータベースから、前記パケットに対応するパラメータを検索する過程と、

前記複数のＩＰセキュリティ処理装置の各々が、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行う過程と、
を備えることを特徴とする請求項１９に記載のパケットに対するＩＰセキュリティ処理方法。
【請求項２１】　前記認証キー交換手段と前記ＩＰセキュリティ処理手段との間におけるパケットの転送を、データリンクレイヤの種別に応じて、最適化する過程を備えることを特徴とする請求項１２乃至２０の何れか一項に記載のパケットに対するＩＰセキュリティ処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば、イントラネットとインターネットとを接続するために使用されるゲートウェイ装置におけるセキュリティーを向上させたセキュリティーゲートウェイ装置に関する。
【０００２】
【従来の技術】インターネットのアプリケーションの一つとして、仮想専用線（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）がある。この仮想専用線においては、インターネット自体のオープン性から、セキュリティの問題があるため、インターネットプロトコル（ＩＰ）にセキュリティー機能を付加するプロトコルであるＩＰセキュリティー（ＩＰ　Ｓｅｃｕｒｉｔｙ：以下「ＩＰｓｅｃ」と記する）によりパケットを暗号化して通信を行うことが必須となっている。
【０００３】図９は従来の信号通信システムの一例のブロック図である。
【０００４】この暗号通信システムにおいては、端末１００ａ－１００ｎからなる第１のグループの各端末に第１の暗号ゲートウェイ装置１１０が接続されており、同様に、端末１２０ａ－１２０ｎからなる第２のグループの各端末に第２の暗号ゲートウェイ装置１３０が接続されている。第１の暗号ゲートウェイ装置１１０と第２の暗号ゲートウェイ装置１３０とはネットワーク１４０を介して相互に接続されている。
【０００５】第１のグループの各端末１００ａ－１００ｎと第２のグループの各端末１２０ａ－１２０ｎとの間の通信において、第１及び第２の暗号ゲートウェイ装置１１０、１３０を介して通信されるパケットデータの暗号化アルゴリズムあるいは暗号化に使用する鍵その他のパラメータは、第１及び第２の暗号ゲートウェイ装置１１０、１３０間においては、固定されている。
【０００６】図９に示すような暗号通信システムにおいては、第１及び第２の暗号ゲートウェイ装置１１０、１３０を通過しないパケットは、本来、復号化されることはない。しかしながら、第１及び第２の暗号ゲートウェイ装置１１０、１３０を接続するネットワーク１４０に

おいては、これらの暗号化されたパケットが傍受され、パケットの暗号化アルゴリズムや鍵を解読されるおそれがある。

【０００７】このようなおそれに対して、例えば、特開平７－１０７０８２号公報は、暗号化または非暗号化の選択またはセッション鍵の選択を端末の組み合わせ毎に、あるいは、セッション毎に設定することができる暗号ゲートウェイ装置を開示している。

【０００８】

【発明が解決しようとする課題】また、ＲＦＣ（Ｒｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔｓ）１８２５－１８２８には、インターネットプロトコル（ＩＰ）におけるセキュリティーを扱った「Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ＩｎｔｅｒｎｅｔＰｒｏｔｏｃｏｌ」（以下「ＩＰｓｅｃ」と呼ぶ）が規定されている。

【０００９】図１０は、ＩＰｓｅｃにおいて規定されているＩＰ用セキュリティ認証ヘッダの一例を示す図である。

【００１０】このＩＰ用セキュリティ認証ヘッダには、このヘッダの次のヘッダの識別子、このヘッダの長さ、ＳＰＩ（Ｓｅｃｕｒｉｔｙ Ｐａｒａｍｅｔｅｒ Ｉｎｄｅｘ）可変長の認証データ（ａｕｔｈｅｎｔｉｃａｔｅｄ ｄａｔａ）が格納されている。このＩＰ用セキュリティ認証ヘッダは、各ＩＰパケットにおいて、ＩＰヘッダとＩＰデータグラムとの間に挿入される。

【００１１】上述したようなパケットの暗号化処理はそれ自体非常に演算処理負荷が高い。このため、専用の暗号ＬＳＩを適用するなどの性能向上がはかられているが、根本的な解決にはなっていないのが現状である。

【００１２】本発明は、このような問題点に鑑みてなされたものであり、パケットを暗号化して通信を行うシステムにおいて、パケットの暗号化に要する演算処理の負荷の集中を防止し、個々のコンポーネントにおける演算処理の負荷を減少させることを可能にするセキュリティーゲートウェイ装置及びパケット処理方法を提供することを目的とする。

【００１３】

【課題を解決するための手段】この目的を達成するため、本発明は、ＩＰセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートするネゴシエーション処理を行う認証キー交換手段と、前記認証キー交換手段と内部通信路で接続されており、前記認証キー交換手段から送られてきたパケットに対してＩＰセキュリティ処理を実行するＩＰセキュリティ処理手段と、からなるセキュリティゲートウェイ装置を提供する。

【００１４】前記ＩＰセキュリティ処理手段は複数のＩＰセキュリティ処理装置からなるものとすることができる。この場合、前記認証キー交換手段は、前記ネゴシエーション処理後に、前記パケットを前記複数のＩＰセキュリティ処理装置の何れかに振り分ける振り分け処理を行い、前記複数のＩＰセキュリティ処理装置の各々は前記認証キー交換手段から振り分けられた前記パケットに対してＩＰセキュリティ処理を実行する。

【００１５】本発明に係るセキュリティゲートウェイ装置においては、ＩＰｓｅｃ通信に必要な２つの機能要素である認証キー交換（Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃｈａｎｇｅ：ＩＫＥ）とＩＰｓｅｃとが別手段として配備され、さらに、ＩＰｓｅｃ通信のバンドルが負荷分散される。これにより、通信スループットをマクロレベルで向上させることが可能となる。

【００１６】さらに、ＩＰセキュリティ処理手段をクラスタ構成とし、すなわち、複数のＩＰセキュリティ処理装置からなるものとすることにより、セキュリティゲートウェイ装置全体のスケーラビリティを確保することが可能となる。

【００１７】前記認証キー交換手段は、ＩＰセキュリティ処理を行うべきパケットを受信した場合には、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットのＩＰセキュリティ処理を行うＩＰセキュリティ処理装置を決定し、前記パケットを前記ＩＰセキュリティ処理装置に転送するものとして構成することができる。

【００１８】前記認証キー交換手段はローカルデータベースを有しているものとして構成することができる。この場合、前記認証キー交換手段は、検索したパラメータと、前記パケットのＩＰセキュリティ処理を行わせることに決定した前記ＩＰセキュリティ処理装置の識別子とを相互にリンク付けした状態で、前記パラメータ及び前記識別子を前記ローカルデータベースに保存することができる。

【００１９】前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記ＩＰセキュリティ処理装置に転送することが好ましい。

【００２０】前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えており、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存するものとして構成することができる。

【００２１】前記認証キー交換手段から前記パケットを受信した前記ＩＰセキュリティ処理装置は、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行うものとして構成することができる。

【００２２】前記認証キー交換手段は前記パケットをカプセル化し、カプセル化した前記パケットを前記ＩＰセキュリティ処理装置に転送するものとして構成すること

ができる。

【００２３】前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えているものとして構成することができる。この場合、前記複数のＩＰセキュリティ処理装置の各々は、前記認証キー交換手段から受信したカプセル化した前記パケットを復元し、前記ローカルデータベースから、前記パケットに対応するパラメータを検索し、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行うこととものとして構成することができる。

【００２４】前記認証キー交換手段並びに前記複数のＩＰセキュリティ処理装置の各々はプロセッサを搭載した基板から構成することができる。この場合、前記認証キー交換手段並びに前記複数のＩＰセキュリティ処理装置の各々は内部バスで相互に接続される。

【００２５】前記認証キー交換手段と前記ＩＰセキュリティ処理手段との間におけるパケットの転送は、データリンクレイヤの種別に応じて、最適化することが可能である。

【００２６】また、本発明は、認証キー交換手段が、ＩＰセキュリティ通信に必要なパラメータを対向するセキュリティゲートウェイとの間でネゴシエートする第１の過程と、前記認証キー交換手段と内部通信路で接続されているＩＰセキュリティ処理手段において、前記認証キー交換手段から送られてきたパケットに対してＩＰセキュリティ処理を実行する第２の過程と、からなるパケットに対するＩＰセキュリティ処理方法を提供する。

【００２７】前記ＩＰセキュリティ処理手段は複数のＩＰセキュリティ処理装置からなるものとして構成することができる。この場合、本方法は、前記第１の過程の後に、前記認証キー交換手段が、前記パケットを前記複数のＩＰセキュリティ処理装置の何れかに振り分ける第３の過程をさらに備え、前記第２の過程においては、前記複数のＩＰセキュリティ処理装置の各々が前記認証キー交換手段から振り分けられた前記パケットに対してＩＰセキュリティ処理を実行するものとして構成することができる。

【００２８】本方法は、前記認証キー交換手段が、ＩＰセキュリティ処理を行うべきパケットを受信した場合に、ネゴシエートしたパラメータの中からそのパケットに対応するパラメータを検索する第４の過程と、検索したパラメータに基づいて、前記パケットのＩＰセキュリティ処理を行うＩＰセキュリティ処理装置を決定する第５の過程と、前記パケットを前記第５の過程において決定した前記ＩＰセキュリティ処理装置に転送する第６の過程と、を備えるものとして構成することができる。

【００２９】前記認証キー交換手段はローカルデータベースを有するものとして構成することができる。この場合、本方法は、前記認証キー交換手段が、検索したパラメータと、前記パケットのＩＰセキュリティ処理を行わせることに決定した前記ＩＰセキュリティ処理装置の識別子とを相互にリンク付けする過程と、前記認証キー交換手段が、前記パラメータ及び前記識別子を前記ローカルデータベースに保存する過程と、を備えることが好ましい。

【００３０】前記第６の過程において、前記認証キー交換手段は、検索したパラメータを前記パケットとともに前記ＩＰセキュリティ処理装置に転送することが好ましい。

【００３１】前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えているものとして構成することができる。この場合、本方法は、前記複数のＩＰセキュリティ処理装置の各々が、前記認証キー交換手段から受信した前記パラメータを前記ローカルデータベースに保存する過程を備えることができる。

【００３２】本方法は、前記認証キー交換手段から前記パケットを受信した前記ＩＰセキュリティ処理装置が、前記ローカルデータベースから、前記パケットに対応するパラメータを検索する過程と、前記ＩＰセキュリティ処理装置が、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行う過程と、を備えることが好ましい。

【００３３】本方法は、前記認証キー交換手段が前記パケットをカプセル化する過程を備えることが好ましく、この場合、前記カプセル化された前記パケットが前記第６の過程において前記ＩＰセキュリティ処理装置に転送されることが好ましい。

【００３４】前記複数のＩＰセキュリティ処理装置の各々はローカルデータベースを備えているものとして構成することができる。この場合、本方法は、前記複数のＩＰセキュリティ処理装置の各々が、前記認証キー交換手段から受信したカプセル化した前記パケットを復元する過程と、前記複数のＩＰセキュリティ処理装置の各々が、前記ローカルデータベースから、前記パケットに対応するパラメータを検索する過程と、前記複数のＩＰセキュリティ処理装置の各々が、検索したパラメータに基づいて、前記パケットに対してＩＰセキュリティ処理を行う過程と、を備えることが好ましい。

【００３５】さらに、本方法は、前記認証キー交換手段と前記ＩＰセキュリティ処理手段との間におけるパケットの転送を、データリンクレイヤの種別に応じて、最適化する過程を備えることができる。

【００３６】

【発明の実施の形態】図１は、本発明の第１の実施形態に係るセキュリティゲートウェイ装置のブロック図である。

【００３７】ＩＰｓｅｃ通信を行う際には、対向装置との間でアルゴリズムや鍵などのＩＰｓｅｃ通信パラメータをネゴシエートするプロトコル（ＩＫＥ）と、ネゴシエートしたパラメータを適用して実際にＩＰｓｅｃ処理

を行うプロトコル（ＩＰｓｅｃ）とが必要となる。

【００３８】このため、本実施形態に係るセキュリティゲートウェイ装置は、図１に示すように、認証キー交換を行う、すなわち、ＩＰｓｅｃ通信パラメータをネゴシエートする認証キー交換処理部１１（以下、「ＩＫＥ処理部１１」と呼ぶ）と、実際にＩＰｓｅｃ処理を行うＩＰｓｅｃ処理部１２の２つのコンポーネントに分割されている。

【００３９】さらに、ＩＰｓｅｃ処理部１２をクラスタ構成とされている。すなわち、ＩＰｓｅｃ処理部１２はｎ個（ｎは２以上の正の整数）のＩＰｓｅｃ処理装置１２ａ－１２ｎから構成されている。

【００４０】ＩＫＥ処理部１１とＩＰｓｅｃ処理部１２とはイーサネット（登録商標）その他の内部通信路１３を介して接続されている。

【００４１】図２は、本実施形態に係るセキュリティゲートウェイ装置のより具体的なブロック図である。

【００４２】図２に示すように、ＩＫＥ処理部１１は対向するセキュリティゲートウェイ（ＳＧＷ）１４とインターネットその他のインセキュアネットワーク１７を介して接続されている。

【００４３】また、ＩＫＥ処理部１１はローカルデータベース１５を内蔵しており、同様に、ＩＰｓｅｃ処理部１２を構成するＩＰｓｅｃ処理装置１２ａ－１２ｎの各々もローカルデータベース１６を内蔵している。

【００４４】次いで、本実施形態に係るセキュリティゲートウェイ装置の動作の概要を以下に説明する。

【００４５】ＩＫＥ処理部１１は、対向するセキュリティゲートウェイ１４との間でＩＫＥプロトコルによりＩＰｓｅｃ通信パラメータをネゴシエートする。ネゴシエートしたパラメータ情報（以後「ＩＰｓｅｃ　ＳＡ」と呼ぶ）を、ローカルデータベース１５に保存するとともに、このＩＰｓｅｃ処理を実際に行うＩＰｓｅｃ処理装置をＩＰｓｅｃ処理装置１２ａ－１２ｎの中から一つ決定する。例えば、ＩＰｓｅｃ処理装置１２ａが決定される。

【００４６】次いで、ＩＰｓｅｃ　ＳＡをＩＰｓｅｃ処理装置１２ａに転送する。同時に、選択したＩＰｓｅｃ処理装置１２ａの識別子を、対応するＩＰｓｅｃ　ＳＡにリンク付ける。

【００４７】ＩＫＥ処理部１１からＩＰｓｅｃ　ＳＡタを受信したＩＰｓｅｃ処理装置１２ａは、そのＩＰｓｅｃ　ＳＡをローカルデータベース１６に保存する。

【００４８】ＩＫＥ処理部１１は、セキュリティゲートウェイ１４からＩＰｓｅｃ処理すべきパケットを受信した場合、そのパケットに対応するＩＰｓｅｃ　ＳＡを検索する。次いで、ＩＫＥ処理部１１は、検索したＩＰｓｅｃ　ＳＡに基づいて、対応するＩＰｓｅｃ処理装置（例えば、ＩＰｓｅｃ処理装置１２ａ）を決定し、受信パケットをＩＰｓｅｃ処理装置１２ａへ転送する。

【００４９】ＩＫＥ処理部１１からＩＰｓｅｃ処理パケットを受信したＩＰｓｅｃ処理装置１２ａは、ローカルデータベース１６から、対応するＩＰｓｅｃ　ＳＡを検索する。ＩＰｓｅｃ処理装置１２ａは、検索したＩＰｓｅｃ　ＳＡに基づいて、実際のＩＰｓｅｃ処理（暗号／復号処理及び認証処理）を実行し、処理済みのパケット１８を出力する。

【００５０】次いで、本実施形態に係るセキュリティゲートウェイ装置の動作をＩＰｓｅｃＳＡ確立フェーズ及びＩＰｓｅｃ通信フェーズの２つのフェーズに分けて、それぞれ図２から図７までを参照して説明する。図２は、ＩＰｓｅｃ　ＳＡ確立フェーズにおける本セキュリティゲートウェイ装置の作動状態を示すブロック図、図３は、ＩＰｓｅｃ通信フェーズにおける本セキュリティゲートウェイ装置の作動状態を示すブロック図、図４は、ＩＰｓｅｃ　ＳＡ確立フェーズにおけるＩＫＥ処理部１１の動作を示すフローチャート、図５は、ＩＰｓｅｃ　ＳＡ確立フェーズにおけるＩＰｓｅｃ処理部１２の動作を示すフローチャート、図６は、ＩＰｓｅｃ通信フェーズにおけるＩＫＥ処理部１１の動作を示すフローチャート、図７は、ＩＰｓｅｃ通信フェーズにおけるＩＰｓｅｃ処理部１２の動作を示すフローチャートである。

【００５１】ＩＰｓｅｃ　ＳＡ確立フェーズにおいては、ＩＫＥ処理部１１が対向するセキュリティゲートウェイ１４との間で、ＩＫＥプロトコルを用いてＩＰｓｅｃ処理に必要な各種パラメータ（アルゴリズム、鍵等）をネゴシエートする（図４のステップＳ４０１）。以後、このネゴシエーション処理の実行をＩＰｓｅｃ　ＳＡ確立と呼ぶ。

【００５２】ＩＰｓｅｃ　ＳＡを確立すると、ＩＫＥ処理部１１は、このＩＰｓｅｃ処理を実際に行うＩＰｓｅｃ処理装置として、クラスタすなわちＩＰｓｅｃ処理装置１２ａ－１２ｎの中から一つのＩＰｓｅｃ処理装置を選択する（図４のステップＳ４０２）。この際、ラウンドロビン等のアルゴリズムにより、クラスタ内の負荷分散を考慮して、ＩＰｓｅｃ処理装置を選択する。ここでは、ＩＰｓｅｃ処理装置１２ｎが選択されたものと想定する。

【００５３】次いで、ＩＫＥ処理部１１は、ＩＰｓｅｃ　ＳＡと選択したＩＰｓｅｃ処理装置１２ｎの識別子とをリンク付けし、双方をローカルデータベース１５に保存する（図４のステップＳ４０３）。例えば、図２に示すように、ローカルデータベース１５には、ＩＰｓｅｃ　ＳＡとしてパラメータ「SA_{21}」、それに対応するＩＰｓｅｃ処理装置としてＩＰｓｅｃ処理装置１２ｎの識別子「２３」がリンク付けされた状態で保存される。

【００５４】次いで、ＩＫＥ処理部１１は、そのＩＰｓｅｃ　ＳＡを、選択したＩＰｓｅｃ処理装置であるＩＰｓｅｃ処理装置１２ｎに転送する（図４のステップＳ４０４）。

【００５５】ＩＫＥ処理部１１からＩＰｓｅｃ　ＳＡ「SA_{21}」を受信したＩＰｓｅｃ処理装置１２ｎは（図５のステップＳ５０１）、そのＩＰｓｅｃ　ＳＡ「SA_{21}」を自らのローカルデータベース１６に保存する（図５のステップＳ５０２）。

【００５６】ＩＰｓｅｃ通信フェーズにおいては、ＩＫＥ処理部１１は対向するセキュリティゲートウェイ１４からパケットを受信すると（図６のステップＳ６０１）、受信したパケットに基づいて、そのパケットを処理すべきＩＰｓｅｃ　ＳＡをローカルデータベース１５から検索する（図６のステップＳ６０２）。例えば、図３に示すように、ローカルデータベース１５には、ＩＰｓｅｃ　ＳＡ「SA_{31}」と、それに対応するＩＰｓｅｃ処理装置の識別子「３３」とが相互にリンク付けされた状態で保存されている。

【００５７】次いで、ＩＫＥ処理部１１はエントリがあるか否かを判定する（図６のステップＳ６０３）。

【００５８】エントリがある場合には（図６のステップＳ６０３のＹＥＳ）、パケットを処理すべきＩＰｓｅｃ処理装置を決定する（図６のステップＳ６０４）。例えば、パケットを処理すべきＩＰｓｅｃ　ＳＡとしてＩＰｓｅｃ　ＳＡ「SA_{31}」が検索された場合には、そのＩＰｓｅｃ　ＳＡ「SA_{31}」に対応するＩＰｓｅｃ処理装置として、識別子「３３」で表されるＩＰｓｅｃ処理装置が決定される。ここでは、識別子「３３」で表されるＩＰｓｅｃ処理装置はＩＰｓｅｃ処理装置１２ｎであるとする。

【００５９】次いで、ＩＫＥ処理部１１は、パケットをＩＰ　ｉｎ　ＩＰ　Ｔｕｎｎｅｌｉｎｇでカプセル化し、カプセル化したパケットをＩＰｓｅｃ処理装置１２ｎに対して転送する（図６のステップＳ６０５）。

【００６０】一方、エントリがない場合には（図６のステップＳ６０３のＮＯ）、受信したパケットを破棄し（図６のステップＳ６０６）、次のパケットの受信を待つ。

【００６１】ＩＰｓｅｃ処理装置１２ｎはＩＫＥ受信部１１からパケットを受信すると（図７のステップＳ７０１）、カプセル化されたパケットを復元する、すなわち、パケットからカプセルを取り外す（図７のステップＳ７０２）。

【００６２】次いで、ＩＰｓｅｃ処理装置１２ｎは、ローカルデータベース１６から、そのパケットに対応するＩＰｓｅｃ　ＳＡを検索する（図７のステップＳ７０３）。

【００６３】次いで、ＩＰｓｅｃ処理装置１２ｎは、エントリが有るか否かを判定する（図７のステップＳ７０４）。

【００６４】エントリが有る場合には（図７のステップＳ７０４のＹＥＳ）、検索したＩＰｓｅｃ　ＳＡに基づいて実際のＩＰｓｅｃ処理（暗号化／復号及び認証）を実行する（図７のステップＳ７０５）。

【００６５】次いで、ＩＰｓｅｃ処理装置１２ｎは、このようにしてＩＰｓｅｃ処理したパケット１９（図３参照）をネットワークへ送出する（図７のステップＳ７０６）。

【００６６】一方、エントリがない場合には（図７のステップＳ７０４のＮＯ）、受信したパケットを破棄し（図７のステップＳ７０７）、次のパケットの受信を待つ。

【００６７】以上のように、本実施形態に係るセキュリティゲートウェイ装置によれば、次のような効果を得ることができる。

【００６８】第一の効果は、処理負荷の高いＩＰｓｅｃ処理からＩＰｓｅｃ　ＳＡ確立処理を分離させることにより、ＩＰｓｅｃ処理のスループットを上げることができる点である。

【００６９】第二の効果は、ＩＰｓｅｃ処理部１２を複数のＩＰｓｅｃ処理装置１２ａ－１２ｎからなるクラスタ構成とすることにより、ＩＰｓｅｃ処理の負荷分散を図り、通信負荷に対して柔軟に対応することができ、スケーラビリティを確保することができる点である。

【００７０】図８は、本発明の第２の実施形態に係るセキュリティゲートウェイ装置の構造を示す概略図である。

【００７１】本実施形態に係るセキュリティゲートウェイ装置においては、第１の実施形態の場合と同様に、ＩＫＥ処理部とＩＰｓｅｃ処理部とはそれぞれ別のコンポーネントとして形成されているが、本実施形態におけるＩＫＥ処理部８１とＩＰｓｅｃ処理部８２とはともにプロセッサ搭載ボードとして形成されており、内部バス８３を介して相互に接続されている。これにより、ＩＫＥ処理部８１とＩＰｓｅｃ処理部８２とは外見上は単一の装置として構成されている。

【００７２】ＩＫＥ処理部８１とＩＰｓｅｃ処理部８２を構成する複数のＩＰｓｅｃ処理装置との間の通信は内部バス８３を経由して行われる。

【００７３】また、ＩＫＥ処理部８１とＩＰｓｅｃ処理部８２との間の通信路においては、データリンクレイヤの種別に応じて、転送方式を最適化することが可能である。

【００７４】例えば、ＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ　Ｔｒａｎｓｆｅｒ　Ｍｏｄｅ：非同期転送モード）を用いる場合、ＩＫＥ処理部８１とＩＰｓｅｃ処理部８２との間をポイントツーポイント（Ｐｏｉｎｔ　ｔｏ　Ｐｏｉｎｔ）の仮想チャネル（Ｖｉｒｔｕａｌ　Ｃｈａｎｎｅｌ：ＶＣ）で接続し、ダイレクトにＬＬＣ／ＳＮＡＰカプセル化することにより、ＩＰ　ｉｎ　ＩＰ　Ｔｕｎｎｅｌｉｎｇのオーバヘッドを軽減することができる。

【００７５】

13

【発明の効果】以上のように、本発明に係るセキュリティゲートウェイ装置によれば、ＩＰｓｅｃ処理のスループットを上げることができるという効果を得ることができる。

【００７６】本発明に係るセキュリティゲートウェイ装置においては、ＩＰｓｅｃ　ＳＡ確立処理とＩＰｓｅｃ処理とが分離されている。具体的には、認証キー交換手段（実施形態におけるＩＫＥ処理部）がＩＰｓｅｃ　ＳＡ確立処理、すなわち、ＩＰセキュリティ通信に必要なパラメータをセキュリティゲートウェイとの間でネゴシエートする処理を行い、ＩＰセキュリティ処理手段（実施形態におけるＩＰｓｅｃ処理部）が認証キー交換手段から送られてきたパケットに対して実際にＩＰセキュリティ処理を実行する。このように、処理負荷の高いＩＰｓｅｃ処理からＩＰｓｅｃ　ＳＡ確立処理を分離させることにより、ＩＰｓｅｃ処理のスループットを上げることが可能である。

【００７７】また、ＩＰｓｅｃ処理部を複数のＩＰｓｅｃ処理装置からなるクラスタ構成とすることにより、ＩＰｓｅｃ処理の負荷分散を図ることができ、高いスケーラビリティを確保することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るセキュリティゲートウェイ装置のブロック図である。

【図２】ＩＰｓｅｃ　ＳＡ確立フェーズにおける、第１の実施形態に係るセキュリティゲートウェイ装置の作動状態を示すブロック図である。

【図３】ＩＰｓｅｃ通信フェーズにおける、第１の実施形態に係るセキュリティゲートウェイ装置の作動状態を示すブロック図である。

【図４】第１の実施形態に係るセキュリティゲートウェイ装置において、ＩＰｓｅｃＳＡ確立フェーズにおけるＩＫＥ処理部の動作を示すフローチャートである。

【図５】第１の実施形態に係るセキュリティゲートウェイ装置において、ＩＰｓｅｃＳＡ確立フェーズにおけるＩＰｓｅｃ処理部の動作を示すフローチャートである。

【図６】第１の実施形態に係るセキュリティゲートウェイ装置において、ＩＰｓｅｃ通信フェーズにおけるＩＫＥ処理部の動作を示すフローチャートである。

【図７】第１の実施形態に係るセキュリティゲートウェイ装置において、ＩＰｓｅｃ通信フェーズにおけるＩＰｓｅｃ処理部の動作を示すフローチャートである。

【図８】本発明の第１の実施形態に係るセキュリティゲートウェイ装置の概略図である。

【図９】従来の信号通信システムの一例のブロック図である。

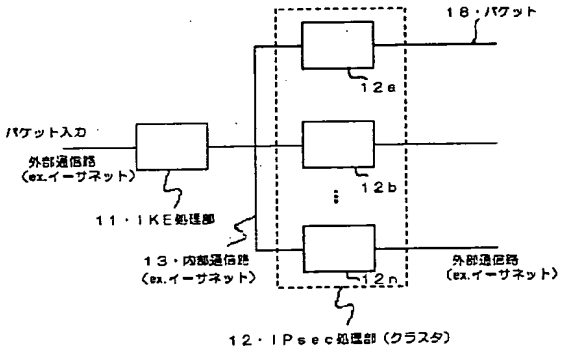
【図１０】ＩＰｓｅｃにおいて規定されているＩＰ用セキュリティ認証ヘッダの一例を示す図である。

【符号の説明】

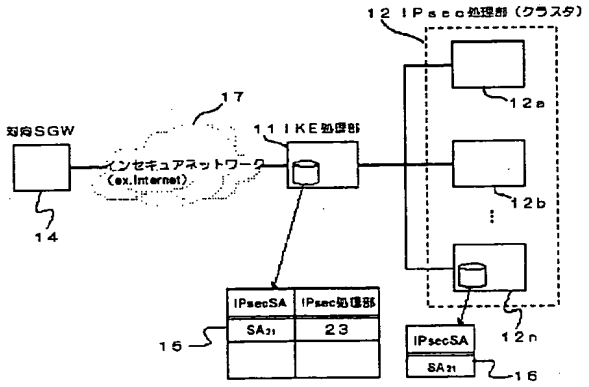
１１　第１の実施形態におけるＩＫＥ処理部
１２　第１の実施形態におけるＩＰｓｅｃ処理部
１２ａ－１２ｎ　ＩＰｓｅｃ処理装置
１３　内部通信路
１４　セキュリティゲートウェイ
１５　ローカルデータベース
１６　ローカルデータベース
１７　インセキュアネットワーク
１８、１９　パケット
８１　第２の実施形態におけるＩＫＥ処理部
８２　第２の実施形態におけるＩＰｓｅｃ処理部
８３　内部バス

14

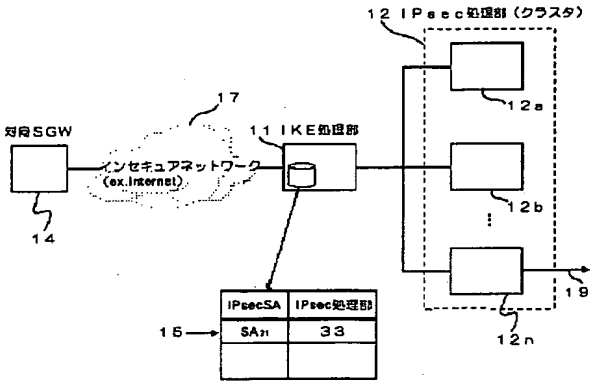
【図１】



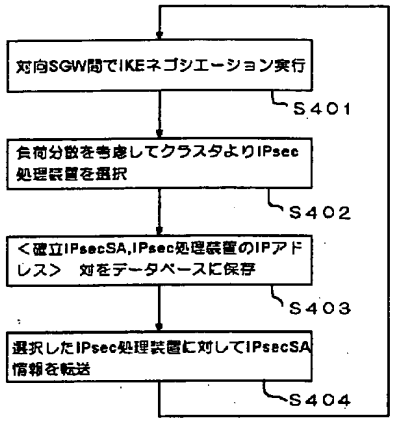
【図２】



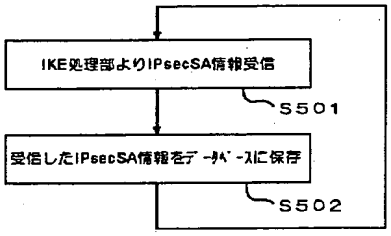
【図３】



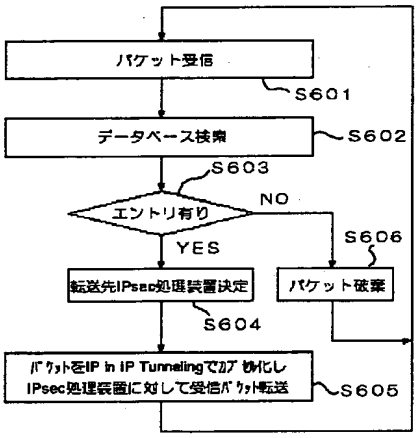
【図４】



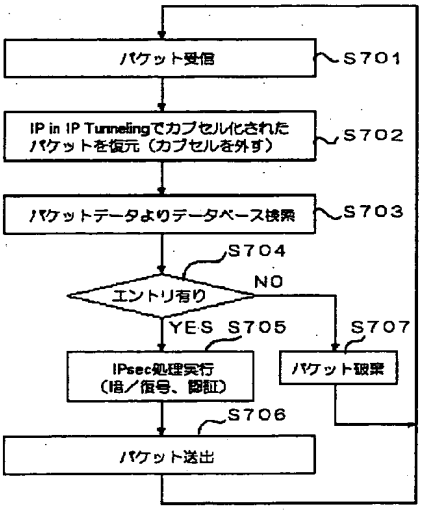
【図５】



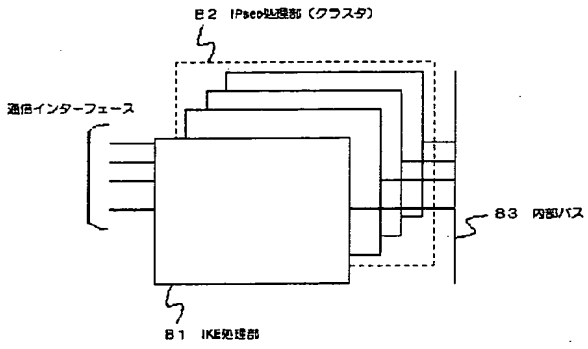
【図６】



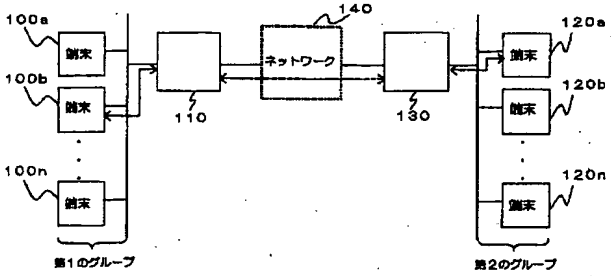
【図７】



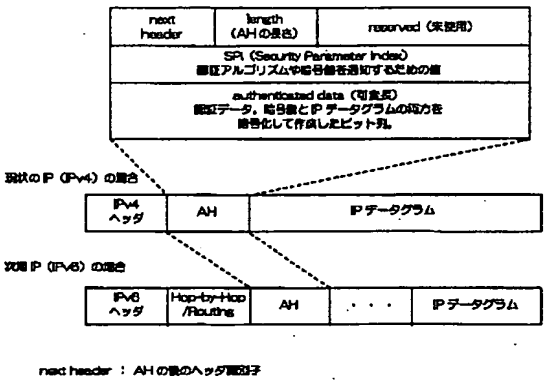
【図８】



【図９】



【図１０】


next header
length (AHの長さ)
reserved (未使用)
SPI (Security Parameter Index)
認証アルゴリズムや暗号鍵を識別するための値
authenticated data (可変長)
認証データ，暗号鍵とIPデータグラムの和から
暗号化して作成したビット列
現状のIP (IPv4) の場合
IPv4 ヘッダ
AH
IPデータグラム
次期IP (IPv6) の場合
IPv6 ヘッダ
Hop-by-Hop /Routing
AH
・・・
IPデータグラム
next header ： AHの後のヘッダ識別子